
**PROTOCOL TO SECURE VULNERABILITY ASSESSMENTS SUBMITTED BY
COMMUNITY WATER SYSTEMS TO EPA**

"Information Protection Protocol"

**Pursuant to Title IV of the Public Health Security and Bioterrorism
Preparedness and Response Act of 2002**

This Protocol is Effective November 30, 2002

November 30, 2002

EXECUTIVE SUMMARY

In June 2002, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) was signed into public law (P.L. 107-188). Title IV of this Act amends the Safe Drinking Water Act and outlines actions community water systems and the U.S. Environmental Protection Agency (EPA) must take to improve the security of the nation's drinking water infrastructure. The Bioterrorism Act requires community water systems serving a population greater than 3,300 persons to conduct, certify the completion of, and submit to EPA an assessment of the vulnerability of the system to terrorist attack or other acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. In turn, EPA is required to handle the submitted vulnerability assessments under strict security arrangements and to develop, by November 30, 2002, in consultation with appropriate federal law enforcement and intelligence officials, the necessary protocols to protect the copies of the assessments.

EPA developed this Information Protection Protocol to safeguard the vulnerability assessments and any information derived from them once these documents are in EPA's custody. This protocol ensures that all assessments are kept in a secure location. Only individuals designated by the EPA Administrator will have access to these documents, and no assessment or "information derived from" a submitted vulnerability assessment will be available to anyone other than those designated, except as specified under Sections 1433(a)(6) and (7) of the Safe Drinking Water Act, as amended.

This protocol builds and expands on EPA's long-standing and excellent track record of handling many types of sensitive information under various environmental statutes and regulations. Throughout the years since EPA's establishment, hundreds of thousands of documents containing sensitive information have been entrusted to EPA. Types of information EPA safeguards include enforcement-confidential information concerning on-going or pending law enforcement efforts, grand jury deliberations, national security information, and information submitted to EPA by regulated business and claimed as confidential. Much of EPA's work involves handling Confidential Business Information (CBI), which contains trade secrets or financial information that if released could harm business interests. EPA has a very stringent training program for protection of such data and uses annual audits and inspections to ensure accountability. No employee has been dismissed for theft of such data.

This protocol establishes a number of protective measures equivalent to those conferred to Secret national security information. The protocol ensures that vulnerability assessments are stored behind closed doors, filed under lock at all times, and accessed only by designated persons under strict security procedures. Vulnerability assessments will be housed at EPA headquarters. A secure review room will be installed and furnished to allow processing of the documents. A document tracking system will allow the vulnerability assessments to be traceable at all times to a single person. Documents will be labeled as sensitive and covered to show that they must be protected. Copying, faxing and loaning of vulnerability assessments will be prohibited except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

An EPA Information Security Manager in headquarters will oversee the protection of the information, manage the day-to-day implementation of the protocol and conduct routine security check-ups. EPA will require a Top Secret clearance for the Headquarters Information Security Manager and a Secret clearance for all other designated individuals. Prior to being designated, potential designees will also undergo security training, and will sign an access agreement which summarizes their responsibilities and personal liabilities if information contained in vulnerability assessments is knowingly or recklessly disclosed. Access will be withdrawn when a designated person terminates employment or no longer requires access because of a change in duties or position. In such cases, the person will be asked to sign a confidentiality agreement prior to termination of access. Each designated person must receive annual refresher security training.

TABLE OF CONTENTS

1 PURPOSE AND DEFINITIONS

- 1.1 Purpose of this Protocol**
- 1.2 Protocol Updates and Revisions**
- 1.3 Definitions**

2 MANDATORY PROTECTIVE MEASURES

- 2.1 Receipt and Tracking**
- 2.2 Cover Sheets for Vulnerability Assessment Information**
- 2.3 Markings to Identify Vulnerability Assessment Information**
- 2.4 Secure File and Review Area**
- 2.5 Storage Equipment**
- 2.6 Custody Rules**
- 2.7 Copying Restrictions and Numbering**
- 2.8 Loaning Vulnerability Assessments to EPA Regional Offices**
- 2.9 Hard Copy Transmissions**
- 2.10 Fax Transmissions**
- 2.11 Discussing Vulnerability Assessment Information on the Telephone**
- 2.12 Use of Electronic Mail (E-Mail)**
- 2.13 Use of Tele-Video Conferences**
- 2.14 Protecting Information Derived from Vulnerability Assessments**
- 2.15 New Non-Sensitive Records**
- 2.16 Use of Stand-Alone Computers**
- 2.17 Use of Home Computers**
- 2.18 Discussing Sensitive Vulnerability Assessment Information in Meetings**
- 2.19 Periodic Security Reviews**
- 2.20 Disposition of New Sensitive Records**

3 DESIGNATIONS AND AUTHORIZED ACCESS PROCEDURES

- 3.1 Designator**
- 3.2 Selection of Designated Persons**
- 3.3 Basic Responsibilities of Designees**
- 3.4 EPA's Headquarters Information Security Manager**
- 3.5 EPA's Regional Security Officers**
- 3.6 Steps in the Designation Process**
 - Step1: Identification of Potential Designees**
 - Step 2: Investigation of Potential Designees**
 - Step 3: Security Training and Evaluation**
 - Step 4: Access Agreement**
 - Step 5: Designation**

- 3.7 Annual Refresher Training**
 - 3.8 Use of Contractors**
 - 3.9 Removal of Designation or Termination of Access**
- 4 REPORTING AND INVESTIGATION OF VIOLATIONS OF PROCEDURES, LOST DOCUMENTS AND UNAUTHORIZED DISCLOSURES**
 - 4.1 Introduction**
 - 4.2 Verbal Reporting**
 - 4.3 Written Reporting**
 - 4.4 Review and Investigation of Written Report**
 - 4.5 Notification to Affected Community Water System**
 - 4.6 Disciplinary Action for EPA Designees Only**
 - 4.7 Criminal Penalties for EPA and non-EPA Designees**

APPENDICES:

- A The Public Health Security and Bioterrorism Preparedness and Response Act of 2002**
- B EPA's Experience in Protecting Sensitive Information**

EXHIBITS:

- A File Log**
- B Cover Sheet for Vulnerability Assessment Information**
- C Stamp for Marking Vulnerability Assessment Records**
- D Loan Request Form**
- E Access Agreement for Designated Individuals**
- F Confidentiality Agreement for Termination of Designation**

CHAPTER 1: PURPOSE AND DEFINITIONS

1.1 Purpose of this Protocol

This "Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA" or Information Protection Protocol, describes the policies and security procedures put in place by EPA to protect from unlawful access and use the copies of vulnerability assessments to be submitted by community water systems.

This protocol is intended to serve as the security manual for individuals to be designated by the EPA Administrator to have access to the vulnerability assessments. It may also inform community water systems as to how EPA will protect and secure their vulnerability assessments.

1.2 Protocol Updates and Revisions

If procedures change for the control, storage, security and handling of vulnerability assessments submitted by community water systems, EPA will update the relevant pages in this protocol and distribute a revised protocol to all designated individuals.

1.3 Definitions

Authorized Access List: A list of those people who the EPA Administrator has designated for access to vulnerability assessments per section 1433 of the Safe Drinking Water Act. Includes the names of the designated individuals, the date of designation, and the date their annual refresher training is due.

Certification: Written notification sent by community water systems to EPA upon completion of a vulnerability assessment required by section 1433(a)(2) of the Safe Drinking Water Act.

Community Water System: As defined in the Safe Drinking Water Act, a community water system is a public water system that (a) serves at least 15 service connections used by year-round residents of the area served by the system, or (b) regularly serves at least 25 year-round residents. The term is generally used in this document to refer to those systems serving a population greater than 3,300 persons that are required to conduct, certify the completion of, and submit to EPA a copy of their vulnerability assessment per section 1433(a)(2) of the Safe Drinking Water Act.

Designated Person or Designee or otherwise authorized individuals: A designated person or designee is an individual designated by the EPA Administrator to have access to vulnerability assessment(s) in accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. An otherwise authorized individual is a person to whom a designated individual is authorized to provide access to vulnerability assessment information under Sections 1433(a)(6) and (7) of the Safe Drinking Water Act.

Information contained in or derived from a Vulnerability Assessment: Information originating from a submitted vulnerability assessment or information generated by EPA as a result of reviewing and analyzing submitted vulnerability assessments.

Information Security Manager: EPA Office of Ground Water and Drinking Water employee in Headquarters assigned to oversee the protection of vulnerability assessment information and implementation of this protocol.

PWSID#: Public Water System Identification Number used by states and EPA in their drinking water regulatory programs.

Regional Security Officer: EPA employee in an EPA Regional office assigned to manage loaned vulnerability assessments and implement this protocol on a regional level.

Vulnerability Assessment or VA: As required under section 1433(a) of the Safe Drinking Water Act, a review of certain specified items to assess the vulnerabilities of the community water system to terrorist attack or other intentional act intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The submitted vulnerability assessment must include, but is not limited to, a review of the following parts of a water system: pipes; constructed conveyances; physical barriers; water collection, pre-treatment, treatment; storage and distribution facilities; electronic, computer or other automated systems; use, storage or handling of chemicals; and system operation and maintenance.

Vulnerability Assessment Information: Used to refer to both vulnerability assessments submitted to EPA and information contained in or derived by EPA from a submitted vulnerability assessment.

Vulnerability Assessment (VA) Tracking Number: Number assigned by EPA to a certification, vulnerability assessment, and information derived from a particular vulnerability assessment, for purposes of tracking its receipt and internal handling. This number may be the PWSID#.

CHAPTER 2: MANDATORY PROTECTIVE MEASURES

EPA will observe the following protective measures in location(s) where vulnerability assessments are kept and secured.

2.1 Receipt and Tracking

A designated individual will transfer vulnerability assessment packages to the Secure File and Review Area where they will be date stamped, covered, marked, assigned a Vulnerability Assessment Tracking Number, and securely filed. EPA may use barcodes for file management and tracking. For each vulnerability assessment, EPA will produce a "File Out" tag that includes the name of the Community Water System, the address, and PWSID# (Exhibit A). EPA will acknowledge receipt of the assessment to the water utility.

2.2 Cover Sheets for Vulnerability Assessment Information

EPA will affix to all vulnerability assessment information a cover sheet (Exhibit B) to distinguish it from other documents.

2.3 Markings to Identify Vulnerability Assessment Information

EPA will mark all vulnerability assessments and any sensitive documents produced in the course of analyzing the vulnerability assessments, with a stamp to identify the sensitivity of the information and as EPA's copy of the vulnerability assessment (Exhibit C). The stamp must be placed on the front of the first page (or on the cover, if the document has one) and on the back of the last page (or back cover, if the document has one). Additionally, EPA may mark other pages as necessary.

2.4 Secure File and Review Area

EPA will designate an area within its facilities in Headquarters to serve as the Secure File and Review Area. Designated individuals will open and process vulnerability assessments in this area only. Only designated individuals will have electronic pass cards and door combinations to grant access to this area. The area will have a secure door with a secure doorframe and doorjamb. As much as possible, EPA will locate this area within already-existing protected areas. EPA may consider the use of intrusion alarms and monitoring cameras as an alternative or in addition to having the Secure File and Review Area within already-protected areas. EPA will place a sign outside the area to clearly convey that only authorized access is permitted.

EPA will furnish the Secure File and Review Area with individual workstations, desk(s), stand-alone computers, chairs, document shredders, electronic date/time stampers, and other supplies as may be necessary.

There may be times when a non-designated individual needs to enter the Secure File and Review Area directly escorted by a designated individual. For example, stand-alone computers may need repair, or the room may need to be cleaned. In such circumstances, a designated individual must ensure that no vulnerability assessment information lies exposed on tables or workstations and that the visitor signs-in upon entry, records his/her contact information, and signs-out upon departure. Designated individuals will accompany non-designated individuals at all times while in the secure area.

2.5 Storage Equipment

EPA may use two types of containers to store vulnerability assessments: metal file cabinets with locking bars and three-way changeable combination locks, or GSA-approved Class 6 security containers used for storing national security information.

2.6 Custody Rules

The authorized recipient of a vulnerability assessment will acknowledge receipt by completing an entry on the "File Out" tag belonging to the particular vulnerability assessment. The entry must contain the printed name, signature, date removed, and time of removal. When returning the document to the file cabinet, the recipient must indicate the date returned, and initial the entry. Refer to Exhibit A for a sample file activity log. When not in use, documents must be returned to the locked file cabinets. EPA will use the individual vulnerability assessment "File-out" tags to trace the custody of documents.

2.7 Copying Restrictions and Numbering

EPA will not copy vulnerability assessments except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

If and when the Office Director authorizes copying, EPA will prepare a watermarked paper and copy the document using this paper to distinguish the copy from the original document submitted by the community water system. EPA will number each copy, track it, cover it and protect it in the same fashion as the submitted vulnerability assessment.

2.8 Loaning Vulnerability Assessments to EPA Regional Offices

EPA Headquarters will not loan vulnerability assessments to Regional offices except on a rare, case-by-case basis as authorized by the Director of the Office of Ground Water and Drinking Water.

If and when the Office Director authorizes a loan to a Regional office, an EPA designated individual in the Regional office will fill out a loan request (Exhibit D), and a

Headquarters designated individual will make a single copy of the vulnerability assessment and transfer it to the Region following the transmittal procedures described below. Both the Headquarters and the Regional designated individuals will retain a copy of the loan request. Loans will be time-limited and extensions may be requested. When a loan expires, EPA Headquarters will obtain the materials back from the EPA Regions. EPA Regions will not be authorized to make copies or keep any sensitive materials. EPA Regions with loaned vulnerability assessments must set in place comparable protective measures as described herein.

2.9 Hard Copy Transmissions

EPA will not transmit hard copies of vulnerability assessments except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

If and when the Office Director authorizes a hard copy transmission, EPA will double-wrap all materials and write the recipient's name and the statement "Sensitive Vulnerability Assessment Information—To be Opened by Addressee Only" in the inner envelope. The outer envelope will only contain the name and address of the recipient, and the direct return address, and be free of any indications that the package contains sensitive vulnerability assessment information.

EPA will send the document using tracked mail such as certified mail, hand-delivery, or other secure method. EPA will require return receipt if certified mail is used. If hand-delivery is used, the carrier must be a designated individual. EPA will not permit the transfer of vulnerability assessments using regular first class mail.

The sender will include a receipt inside the package identifying the contents of the package. The recipient will sign the receipt and send it back to the sender within five days of receipt, to verify receipt and contents. The sender will retain all receipts received for auditing. The sender must also obtain a receipt from the courier service employee who picks up the package.

2.10 Fax Transmissions

EPA will not transmit vulnerability assessments by fax except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

If and when the Office Director authorizes a fax transmission, EPA will use only fax machines with secured lines.

2.11 Discussing Vulnerability Assessment Information on the Telephone

Designated or otherwise authorized individuals may discuss vulnerability assessment information on the telephone only if the transfer of information can not be accomplished in person. In such circumstances, designated individuals should use an encrypted telephone line if available. Under no circumstances may designated persons leave messages containing vulnerability assessment information on voice mail.

2.12 Use of Electronic Mail (E-Mail)

EPA does not authorize the use of email or any other electronic mail system to transmit vulnerability assessment information.

2.13 Use of Tele-Video Conferences

EPA headquarters and EPA regional offices may display and discuss vulnerability assessment information during tele-video conferences. All attendants must be designated or otherwise authorized individuals. If available, compressed video encryption will be used.

2.14 Protecting Information Derived from Vulnerability Assessments

EPA will protect information derived from submitted vulnerability assessments in the same fashion as submitted vulnerability assessments.

2.15 New Non-Sensitive Records

In the course of conducting work activities relating to drinking water security, designated individuals and other EPA staff may obtain information, such as briefing documents, on drinking water system vulnerabilities that have not been derived from the vulnerability assessments submitted to EPA. For example, a designated individual may attend a conference or a workshop and be voluntarily handed information related to water security. EPA staff may also take notes on such presentations. EPA will consider these records, such as handouts and notes, to be personal working papers that need not be protected as strictly as submitted vulnerability assessment information.

2.16 Use of Stand-Alone Computers

Designated individuals may not use computers connected to EPA networks or the Internet, but may use stand-alone computers in the Secure File and Review Area to track submission of the certifications and aggregate data to conduct analysis of vulnerability assessments. There will be no electronic version of vulnerability

assessments, and no information derived from vulnerability assessments will be kept in electronic systems with public access.

2.17 Use of Home Computers

EPA will not authorize the use of home computers in connection with vulnerability assessment information.

2.18 Discussing Sensitive Vulnerability Assessment Information in Meetings

A check to determine that all meeting participants have been designated will precede any discussion of information pertaining to vulnerability assessments. The chair of any meeting that involves a discussion of vulnerability assessment information must ensure that only designated or otherwise authorized individuals are present. At the close of the meeting, the chair of the meeting must ensure all sensitive information, including materials produced at the meeting, is secured.

2.19 Periodic Security Reviews

The Headquarters Information Security Manager (and Regional Security Officers in EPA Regions where vulnerability assessments are on loan) will conduct periodic security inspections/reviews to ensure security practices are being followed. Those who conduct the security reviews will promptly document the results and share them with the Director of EPA's Office of Ground Water and Drinking Water or his/her delegate.

2.20 Disposition of New Sensitive Records

EPA will destroy by shredding, pulverizing or burning, any dated or no longer needed sensitive documents produced in the course of analyzing the vulnerability assessments consistent with EPA's obligations under the Federal Records Act.

CHAPTER 3: DESIGNATIONS AND AUTHORIZED ACCESS PROCEDURES

3.1 Designator

The Bioterrorism Act authorizes the EPA Administrator to designate those individuals who will have access to the vulnerability assessments.

3.2 Selection of Designated Persons

The EPA Administrator will designate those individuals determined to need access to the vulnerability assessments. The EPA Assistant Administrator for Water and the EPA Regional Administrators will identify individuals to be designated based on the following criteria:

- Role in handling and reviewing the vulnerability assessments, and implementing the Bioterrorism Act; and
- Knowledge of community water systems and vulnerability assessment methodologies.

An EPA employee may decline designation.

3.3 Basic Responsibilities of Designees

Every designated person must protect and safeguard any vulnerability assessment information at all times and in compliance with this protocol, not discuss sensitive information with anyone who is not a designated individual or otherwise authorized under Section 1433, and promptly report any apparent violation of access to the Headquarters Information Security Manager.

EPA recognizes that situations not covered by this protocol may arise. In such cases, the Headquarters Information Security Manager will be available for guidance, and each designated person will ensure through personal conduct and accountability that he or she will act consistently with these guidelines to protect, to the best of his or her ability, all vulnerability assessment information.

3.4 EPA's Headquarters Information Security Manager

EPA will assign a designated person to be the **"Information Security Manager."** This person will oversee the protection of vulnerability assessment information and the implementation of this protocol. The Headquarters Information Security Manager will:

- Be the focal point for protection of community water system vulnerability assessment information in EPA
- Maintain the Vulnerability Assessment Tracking System

- Arrange and conduct security briefings of potential designees, and conduct refresher training
- Issue and safeguard the original signed Access Agreements
- Maintain an updated Authorized Access List of designated persons
- Conduct periodic announced and unannounced security inspections for conformance with this protocol, and investigate any reported breaches of security
- Approve contractor security plans in consultation with the appropriate EPA Contract Project Officer, if applicable
- If needed, oversee the vulnerability assessment loan system and keep a record of the loan requests

3.5 EPA's Regional Security Officers

If the Director of EPA's Office of Ground Water and Drinking Water authorizes loaning a vulnerability assessment(s) to an EPA Regional office, the Region will assign a designated employee to become the **"Regional Security Officer."** This person will become the focal point for management of loaned vulnerability assessment(s) at the EPA Regional office level, and follow comparable security operations as those implemented centrally in EPA Headquarters by the Headquarters Information Security Manager. Regional Security Officers will have the following responsibilities:

- Be the focal point for protection of loaned vulnerability assessments at the Regional level
- Oversee the implementation of this protocol among designated individuals
- Maintain an updated record of all designated persons within the Region, to update the official Authorized Access List
- Arrange and conduct security briefings of potential designees in the Region, in consultation with the Headquarters Information Security Manager, and conduct refresher security training
- Conduct security inspections periodically, in consultation with the Headquarters Information Security Manager
- Respond to Headquarters Information Security Manager requests.

3.6 Steps in the Designation Process

Step 1: Identification of Potential Designees

The EPA Assistant Administrator for Water and the EPA Regional Administrators will identify individuals to be designated based on the criteria in section 3.2 of this Protocol.

Step 2: Investigation of Potential Designees

EPA will require a Top Secret clearance for the Headquarters Information Security Manager and a Secret clearance for all other designated individuals, including any Regional Security Officers.

The EPA Administrator may designate individuals pending completion of their security clearance process. Temporary designations will be withdrawn if designated individuals do not complete the clearance process successfully.

Step 3: Security Training and Evaluation

The Headquarters Information Security Manager (or the Regional Security Officer) will train potential designees on the Bioterrorism Act and the procedures described in this protocol. At this time the potential designee will obtain a copy of this protocol. The Headquarters Information Security Manager may ask the potential designee several questions to reinforce the material and ability to implement this protocol.

Step 4: Access Agreement

After successful completion of the security training, the potential designee will sign an Access Agreement (Exhibit E) indicating an understanding and acceptance of the terms and responsibilities. The Headquarters Information Security Manager will also sign the Access Agreement to indicate the designated person was trained and understands the material conveyed. If the designated person is an EPA employee, the direct supervisor of the designated person also signs the Access Agreement.

Step 5: Designation

Designation is effective upon the EPA Administrator's official recognition of the individual as a designated person in the form of a signed Memorandum. Upon designation, the Headquarters Information Security Manager will add the persons' name to the Authorized Access List. The list will be used to control access to the vulnerability assessment information and includes the names of designated individuals, the date of designation, and the date their annual refresher training is due.

3.7 Annual Refresher Training

Each designated person must receive an annual refresher training.

3.8 Use of Contractors

If EPA enters into a contractual relationship in order to carry out its mandate under the Bioterrorism Act, and contract employees need to be designated, these employees will be required to follow EPA procedures and implement this protocol as any designated

individual. As described above, EPA will also require a Secret level clearance for contractors.

3.9 Removal of Designation or Termination of Access

EPA will withdraw designations when the individual no longer requires access to vulnerability assessments because of a change in duties or position. An individual may also be withdrawn, for example, if found not to be adhering to security procedures, or if he or she fails to attend the annual security training. Prior to the designation being relinquished or withdrawn, the designated individual must complete the "Confidentiality Agreement for Termination of Access" (Exhibit F) in accordance with the "Access Agreement" signed prior to designation, and return to the Headquarters Information Security Officer any electronic entry cards to the Secure File and Review Area.

CHAPTER 4: REPORTING AND INVESTIGATION OF VIOLATIONS OF PROCEDURES, LOST DOCUMENTS AND UNAUTHORIZED DISCLOSURES

4.1 Introduction

All designated individuals must report possible violations of security procedures, the loss or misplacement of vulnerability assessment information, and any unauthorized disclosure of materials immediately to the Headquarters Information Security Manager.

For designated EPA employees, the security procedures in this protocol are enforceable by disciplinary actions, set forth in this chapter, in addition to criminal penalties. For designated non-EPA employees, only criminal penalties are enforceable per section 1433 of the Safe Drinking Water Act.

4.2 Verbal Reporting

Any designated individual (EPA employee or not) should provide verbal notice to the Headquarters Information Security Manager within one working day if it is possible that

- Security procedures have been violated
- Vulnerability Assessment materials have been lost or misplaced
- A non-designated person who is not otherwise authorized under Section 1433 has obtained access to vulnerability assessment information.

4.3 Written Reporting

Within two working days, any designated individual (EPA employee or not) should follow up the verbal report with a written report. The written report must describe the possible violation of procedures, the unauthorized disclosure of information, and the materials believed lost or misplaced. It must also include a description of any relevant circumstances or facts known by the designee.

The designee may examine files and discuss the matter with the Headquarters Information Security Manager or the Regional Security Officer. However, only the Headquarters Information Security Manager will be authorized to conduct interviews, review logs, and carry out a detailed investigation.

4.4 Review and Investigation of Written Report

The Headquarters Information Security Manager will inform the Director of EPA's Office of Ground Water and Drinking Water if an incident has occurred. The Office Director will then assign an individual to investigate the incident and to determine if a violation of procedures, loss of information or unauthorized disclosure has occurred.

If the investigation reveals any evidence of a knowing and reckless disclosure of vulnerability assessment information, the Office Director will immediately refer the matter to the appropriate individuals.

4.5 Notification to Affected Community Water System

If the Director of EPA's Office of Ground Water and Drinking Water determines that an unauthorized disclosure occurred, or vulnerability assessment information is missing, EPA will notify the affected community water system(s). The written notice will contain a description of the incident and the date of disclosure, if known.

4.6 Disciplinary Action for EPA Designees Only

[Reserved.]

4.7 Criminal Penalties for EPA and non-EPA Designees

The Director of EPA's Office of Ground Water and Drinking Water will notify the appropriate individuals if a designated person knowingly or recklessly releases or discloses vulnerability assessment information to any unauthorized person. The designated individual who disclosed the information is subject to criminal prosecution and fines in accordance with provisions of chapter 227, 18 United States Code, applicable to class A misdemeanors, and upon conviction may be imprisoned for not more than one year, or both. A convicted EPA employee will also be removed from Federal office or employment.

APPENDIX A: The Public Health Security and Bioterrorism Preparedness and Response Act of 2002

In June 2002, the President signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Title IV of this Act amends the Safe Drinking Water Act (SDWA) by adding new sections 1433 through 1435 which outline actions community water systems and the U.S. Environmental Protection Agency (EPA) must take to improve the security of the nation's drinking water infrastructure. For Title IV of the Bioterrorism Act, consult Public Law 107-188.

Actions required of Community Water Systems

The Bioterrorism Act requires each community water system serving a population greater than 3,300 persons to conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. A vulnerability assessment must include but is not limited to a review of certain specified items (e.g., pipes; constructed conveyances; physical barriers; water collection, pre-treatment, treatment; storage and distribution facilities; electronic, computer or other automated systems; use, storage or handling of chemicals; and system operation and maintenance).

After completion of each vulnerability assessment, each community water system must certify to the EPA Administrator that the assessment has been conducted, and submit a written copy of its assessment to EPA. These requirements are phased-in depending on the size of the community water system.

POPULATION SERVED BY COMMUNITY WATER SYSTEM	DEADLINE FOR CERTIFYING AND SUBMITTING VULNERABILITY ASSESSMENT
100,000 or more persons	March 31, 2003
50,000 to 99,999 persons	December 31, 2003
3,301 to 49,999 persons	June 30, 2004

Small community water systems serving a population of 3,300 or less persons are to be provided guidance by EPA on how to conduct a vulnerability assessment, among other things. However, small systems are not required to prepare a vulnerability assessment or submit it to EPA.

Actions required of EPA

EPA is required to handle all submitted information under strict security arrangements and to develop protocols as may be necessary to protect the copies of the assessments and information derived from the assessments, from unauthorized disclosure. The protocols must be developed prior to November 30, 2002, in consultation with appropriate federal law enforcement and intelligence officials.

The protocols must ensure that: (a) each vulnerability assessment is kept in a secure location; (b) only individuals designated by the EPA Administrator have access to these vulnerability assessments; and (c) no vulnerability assessment or part of an assessment, or information contained in or derived from an assessment, is available to anyone other than the designated individuals, with some exceptions noted below.

Designations, FOIA exemption, and disclosure considerations

The Bioterrorism Act authorizes the EPA Administrator to designate those individuals who will have access to the copies of the vulnerability assessments submitted to EPA. Generally, only these individuals may have access to this information, and no copy, part or information contained or derived from a vulnerability assessment will be generally available to anyone other than those designated by the Administrator.

Information provided to EPA under section 1433 and any information derived therefrom, is exempt from disclosure under the Freedom of Information Act, or FOIA, Title 5 United States Code section 552. The only exception is for information that specifies the system submitting the certification and the date of the certification.

Furthermore, the Bioterrorism Act addresses the situation where a state or local FOIA requirement could be 'triggered' by submission of a written copy of vulnerability assessment to EPA. The Act provides that no community water system will be compelled to submit a copy of its assessment to any governmental entity occasioned by the requirement that the system submit such an assessment to EPA.

The only allowed exceptions for disclosure of vulnerability assessment information by designated individuals is for use in any administrative or judicial proceeding to impose a penalty for failure to comply with the security provisions, and for specific actions under identified sections of the Safe Drinking Water Act; namely, sections 1445 (records and inspections) and 1431 (emergency powers). In addition, no information may be withheld from Congress or from any committee or subcommittee of Congress.

Designated U.S. government employees may discuss the contents of a vulnerability assessment with a state or local official.

Personal liabilities and penalties

Any *designated* person who knowingly or recklessly reveals vulnerability assessment information is subject to criminal prosecution and fines in accordance with provisions of chapter 227, 18 United States Code, applicable to class A misdemeanors, and upon conviction may be imprisoned for not more than one year, or both. A convicted employee will also be removed from Federal office or employment.

APPENDIX B: EPA's Experience in Protecting Sensitive Information

Since the establishment of the Agency in December 1970, hundreds of thousands of documents containing sensitive information have been entrusted to EPA.

Under the Clean Water Act, EPA protects confidential trade secret data on the production, treatment and discharge of wastewater. Approximately 10,000 records over the past 10 years have gone through EPA's Office of Water security program. Only a few records have been reported missing and after extensive investigation in each case, the Agency concluded that there was a high probability of their having been destroyed. Following these instances, immediate corrective measures were taken, including the requirement of monthly reports to track all Confidential Business Information (CBI) transmittals.

Various other environmental statutes and regulations provide a framework for EPA to protect sensitive information, including:

- Toxic Substances Control Act (TSCA): protects CBI on chemical formulas for new and existing chemical products, the volume of chemicals produced, industrial processes used to make particular substances, and financial information about chemicals a company plans to produce;
- Resource Conservation and Recovery Act (RCRA): protects information about the content of waste streams which could potentially be used by competitors to determine what substances a company manufactures;
- Comprehensive Environmental Response, Compensation and Liability Act (CERCLA or Superfund) and the Emergency Planning and Community Right-to-Know Act (EPCRA): secures information about emergency planning and hazardous chemical inventories;
- Federal Insecticide, Fungicide and Rodenticide Act (FIFRA): safeguards chemical formulas, production volume as well as health and safety data about pesticides;
- Clean Air Act (CAA): protects emission production and consumption data, information from engine manufacturers, sales volumes by vehicle class, and information relating to fuel or fuel additive registrations.

The volume of information handled and kept secure by EPA in TSCA alone is significant: 5370 original submissions containing TSCA CBI were processed in Fiscal Year 2001. A total of 145,000 documents (originals and copies) are currently on file under this program. There is also a significant microfiche collection probably numbering in the hundreds of thousands of individual fiche. Approximately 1500 persons including EPA, contractors, and other Federal agencies' employees have access to FIFRA CBI and our track record for securing FIFRA sensitive information is unblemished. There have been no reported cases of compromise in the thousands of documents that are handled weekly under FIFRA. The Agency has a very stringent training program for protection of such data and annual audits and inspections ensure accountability. No employee has been dismissed for theft of such data and very few disclosures or releases of such information to outside sources have occurred. In the late 1970's, EPA's procedures for protecting TSCA CBI were closely scrutinized when the Polaroid Corporation challenged

EPA's potential disclosure of chemical formulations (*Polaroid Corporation v. Costle*, 11 *Envir. Rep. Cas (BNA)* 213 (D. Mass 1978)). In response, EPA agreed to adopt new rules for protecting TSCA CBI, and the U.S. District Court of the District of Massachusetts subsequently issued a Consent Order that required EPA to implement an enhanced system for tracking the information, among other actions.

EXHIBIT A

FILE LOG

VA TRACKING NUMBER: _____

Printed Name	Affiliation (e.g., EPA)	Signature	Date Removed	Date Returned	Initials

This sheet is to remain on the file drawer while the document is in use. It is meant to identify which files have been removed and to assist with re-filing. Thank you.

EXHIBIT B

**THIS MATERIAL CONTAINS
SENSITIVE
VULNERABILITY ASSESSMENT
INFORMATION**

STOP

**You are not to review this information unless you are specifically
designated or otherwise authorized to do so.**

DOES NOT CONTAIN NATIONAL SECURITY INFORMATION (EO 12356)

Only individuals designated by the EPA Administrator may have access to this information in accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Title IV of this Act amends the Safe Drinking Water Act.

The attached information is not to be published, reproduced, publicly discussed, or included in response to a Freedom of Information request (FOIA) or otherwise released to non-designated or otherwise authorized individuals.

The Bioterrorism Act provides for fines, criminal penalties and imprisonment for knowingly or recklessly disclosing vulnerability assessment information to non-designated or otherwise authorized persons. Disclosure may also lead to removal from federal office or employment.

EXHIBIT C

EPA's COPY

**SENSITIVE
WATER VULNERABILITY ASSESSMENT
INFORMATION**

EXHIBIT D

**LOAN REQUEST
VUNERABILITY ASSESSMENT**

Requestor:

Name:

Position:

Date of Request:

What Record is Needed:

Purpose of the Request:

Acknowledgement of Physical Security for the Record, when received:

Estimated Period of Requirement:

ACKNOWLEDGEMENT OF RETURNED LOANED DOCUMENTS

Receiver:

Name:

Position:

Date of Return:

Record Returned:

EXHIBIT E**DRAFT ACCESS AGREEMENT*****For Vulnerability Assessments and Information Derived from Vulnerability Assessments
DESIGNATED INDIVIDUALS******1. Person for whom access is being requested:***_____
Last Name, First Name, Middle Initial_____
Office Phone No._____
Email Address***Organization:******EPA Office/Region:******2. Type of Request (circle):****New**Refresher**Name Change**Organizational Change****3. Confidentiality Agreement:***

I understand that I will have access to certain sensitive information contained in vulnerability assessments submitted to EPA under section 1433 of the Safe Drinking Water Act. I will have access in connection with my official duties on behalf of the U.S. Government, State, County or Local Government, or other organization.

I agree to protect this information from disclosure while it is in my custody. I will not permit this information to come into the possession of any person except in accordance with section 1433 of the Safe Drinking Water Act, and I will route or transmit this information to other authorized persons only via official transfer procedures as set forth in the "Protocols to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA."

I understand that section 1433 of the Safe Drinking Water Act provides for fines and/or imprisonment for knowingly or recklessly disclosing vulnerability assessment information to unauthorized persons. I also understand that I may be subject to criminal penalties in accordance with the 18 USC Chapter 227 for willfully, concealing, misrepresenting, or falsifying facts in this agreement. I also understand that I may be removed from federal office or employment if I knowingly or recklessly disclose this information.

I agree to sign a "Confidential Agreement for Termination or Transfer" if I no longer require access to vulnerability assessments because of a change in duties or position.

I acknowledge I have been trained on the "Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA" and that I fully understand it.

Signature_____
Date***4. The above person has been trained in accordance with the "Protocol To Secure Vulnerability Assessments Submitted by Community Water Systems to EPA".***_____
Printed Name & Signature of Headquarters Information Security Manager_____
Date***5. I certify that the above person needs access to vulnerability assessment information.***_____
Printed Name & Signature of Direct Supervisor_____
Date

EXHIBIT F

DRAFT

CONFIDENTIALITY AGREEMENT FOR TERMINATION OF DESIGNATION

In accordance with my official duties, I have had access to information contained in vulnerability assessments submitted by community water systems to EPA under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Title IV of this Act amends the Safe Drinking Water Act.

Because of a change in duties or position, I no longer require access to this information.

I understand that vulnerability assessment information may not be disclosed except as authorized by the Bioterrorism Act.

I certify that I have returned all vulnerability assessment information in my custody to the Headquarters Information Security Manager as specified in the "Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA."

I certify that I have not removed any documents from the Secure File and Review Room upon my termination.

I further agree that I will not disclose any vulnerability assessment information to any person upon my termination.

I understand that as a person who has had access, I am liable for imprisonment for up to a year, and/or fines and criminal prosecution in accordance with 18 USC, chapter 227, if I knowingly or recklessly disclose this information. Additionally, I understand that revealing this information may lead to removal from federal office or employment.

_____ Full Name (print)	_____ Badge/ID Number
_____ Office Affiliation	_____ Contractor Name and No. (if applicable)
_____ Signature	_____ Date
_____ Signature of Headquarters Security Manager of Regional Security Officer	_____ Date